

A PROBABILISTIC APPROACH TO VALUE SETS OF POLYNOMIALS OVER FINITE FIELDS

ZHICHENG GAO AND QIANG WANG

ABSTRACT. In this paper we study the distribution of the size of the value set for a random polynomial with degree at most $q - 1$ over a finite field \mathbb{F}_q . We obtain the exact probability distribution and show that the number of missing values tends to a normal distribution as q goes to infinity. We obtain these results through a study of a random r -th order cyclotomic mappings. A variation on the size of the union of some random sets is also considered.

1. INTRODUCTION

Let \mathbb{F}_q be the finite field of q elements with characteristic p . Let γ be a fixed primitive element of \mathbb{F}_q throughout the paper. The *value set* of a polynomial g over \mathbb{F}_q is the set V_g of images when we view g as a mapping from \mathbb{F}_q to itself. Clearly g is a *permutation polynomial* (PP) of \mathbb{F}_q if and only if the cardinality $|V_g|$ of the value set V_g is q . Asymptotic formulas such as $|V_g| = \lambda(g)q + O(q^{1/2})$, where $\lambda(g)$ is a constant depending only on certain Galois groups associated to g , can be found in Birch and Swinnerton-Dyer [2] and Cohen [8]. Later, Williams [24] proved that almost all polynomials g of degree d satisfy $\lambda(g) = 1 - \frac{1}{2!} + \frac{1}{3!} + \cdots + (-1)^{d-1} \frac{1}{d!}$.

There are also several results on explicit upper bound for $|V_g|$ if g is not a PP over \mathbb{F}_q ; see for example [14, 19, 20]. Perhaps the most well-known result is due to Wan [20] who proved that if a polynomial g of degree d is not a PP then

$$(1) \quad |V_g| \leq q - \frac{q-1}{d}.$$

On the other hand, it is easy to see that $|V_g| \geq \lceil q/d \rceil$ for any polynomial g over \mathbb{F}_q with degree d . The polynomials achieving this lower bound are called *minimal value set polynomials*. The classification of minimal value set polynomials over \mathbb{F}_{p^k} with $k \leq 2$ can be found in

2000 *Mathematics Subject Classification.* 05A16, 60E05, 11T06.

Key words and phrases. polynomials, value sets, normal distribution, finite fields.

Research of authors was partially supported by NSERC of Canada.

[6, 15], and in [3] for all the minimal value set polynomials in $\mathbb{F}_q[x]$ whose value set is a subfield of \mathbb{F}_q . See [10, 21] for further results on lower bounds of $|V_g|$ and [13] for some classes of polynomials with small value sets. More recently, algorithms and complexity in computing $|V_g|$ have been studied in [7].

We note that all of these results mentioned above relate $|V_g|$ to the degree d of g . It is also well known that every polynomial g over \mathbb{F}_q such that $g(0) = b$ has the form $ax^r f(x^s) + b$ with some positive integers r, s such that $s \mid q - 1$. There are different ways to choose r, s in the form $ax^r f(x^s) + b$. However, in [1], the concept of the index of a polynomial was first introduced and any non-constant polynomial $g \in \mathbb{F}_q[x]$ of degree $\leq q - 1$ can be written *uniquely* as $g(x) = a(x^r f(x^{(q-1)/\ell})) + b$ with index ℓ defined below. Namely, write

$$g(x) = a(x^n + a_{n-i_1}x^{n-i_1} + \cdots + a_{n-i_k}x^{n-i_k}) + b,$$

where $a, a_{n-i_j} \neq 0, j = 1, \dots, k$. The case that $k = 0$ is trivial. Thus, we shall assume that $k \geq 1$. Write $n - i_k = r$, the vanishing order of x at 0 (i.e., the lowest degree of x in $g(x) - b$ is r). Then $g(x) = a(x^r f(x^{(q-1)/\ell})) + b$, where $f(x) = x^{e_0} + a_{n-i_1}x^{e_1} + \cdots + a_{n-i_{k-1}}x^{e_{k-1}} + a_r$,

$$\ell = \frac{q-1}{\gcd(n-r, n-r-i_1, \dots, n-r-i_{k-1}, q-1)} := \frac{q-1}{s},$$

and $\gcd(e_0, e_1, \dots, e_{k-1}, \ell) = 1$. The integer $\ell = \frac{q-1}{s}$ is called the *index* of $g(x)$. From the above definition of index ℓ , one can see that the greatest common divisor condition makes ℓ minimal among those possible choices.

Clearly, the study of the value set of g over \mathbb{F}_q is equivalent to studying the value set $x^r f(x^{(q-1)/\ell})$ over \mathbb{F}_q with index ℓ . Recently Mullen, Wan and Wang [17] used an index approach to study the upper bound of the value set for any polynomial which is not a PP. They proved that if g is not a PP then

$$(2) \quad |V_g| \leq q - \frac{q-1}{\ell}.$$

This result improves Wan's result when the index ℓ of a polynomial is strictly smaller than the degree d . We note that the index ℓ of a polynomial is always smaller than the degree d as long as $\ell \leq \sqrt{q} - 1$.

The above result is obtained through a study of cyclotomic mapping polynomials which were studied earlier in [11, 18, 22]. The index of a polynomial is closely related to the concept of the least index of a cyclotomic mapping polynomial. Recall that γ is a fixed primitive element of \mathbb{F}_q . Let $\ell \mid q - 1$ and the set of all nonzero ℓ -th powers be

C_0 . Then C_0 is a subgroup of \mathbb{F}_q^* of index ℓ . The elements of the factor group \mathbb{F}_q^*/C_0 are the *cyclotomic cosets*

$$C_i := \gamma^i C_0, \quad i = 0, 1, \dots, \ell - 1.$$

For any $a_0, a_1, \dots, a_{\ell-1} \in \mathbb{F}_q$ and a positive integer r , the r -th order cyclotomic mapping $f_{a_0, a_1, \dots, a_{\ell-1}}^r$ of index ℓ from \mathbb{F}_q to itself (see Niederreiter and Winterhof in [18] for $r = 1$ or Wang [22]) is defined by

$$(3) \quad f_{a_0, a_1, \dots, a_{\ell-1}}^r(x) = \begin{cases} 0, & \text{if } x = 0; \\ a_i x^r, & \text{if } x \in C_i, \quad 0 \leq i \leq \ell - 1. \end{cases}$$

It is shown that r -th order cyclotomic mappings of index ℓ produce the polynomials of the form $x^r f(x^s)$ where $s = \frac{q-1}{\ell}$. Indeed, the polynomial presentation is given by

$$g(x) = \frac{1}{\ell} \sum_{i=0}^{\ell-1} a_i x^r \sum_{j=0}^{\ell-1} \zeta^{-ji} x^{js},$$

where $\zeta = \gamma^s$ is a fixed primitive ℓ -th root. On the other hand, as we mentioned earlier, each polynomial $f(x)$ such that $f(0) = 0$ with index ℓ can be written as $x^r f(x^{(q-1)/\ell})$, which is an r -th order cyclotomic mapping with the least index ℓ such that $a_i = f(\zeta^i)$ for $i = 0, \dots, \ell - 1$.

In this paper, we are interested in the probability distribution of the value set size of a random r -th order cyclotomic mapping polynomial for any given index ℓ and any positive integer r , as defined in Equation (3). Thus this enables us to derive the probability distribution of the size of value set of a random polynomial of degree $d \leq q - 1$ over a finite field. In Section 2 we outline our method and a crucial result on normal distribution which is used in this paper. Essentially, we are interested in the distribution of the size of the union of subsets, namely, the distribution of the random variable $X_{t\ell} = |\cup_{j=1}^{\ell} A_j|$ where $A_j = g(C_{j-1})$ for $j = 1, \dots, \ell$ and $t = (r, s)$. In Section 3, we first consider a simplified model such that none of a_i 's in Equation (3) is zero. Hence a_i 's are chosen independently at random from \mathbb{F}_q^* . This means that the zero is not contained in any one of the subsets A_j 's. In particular, in Theorem 1 we obtain the distribution of the number of missing values for a random r -th order cyclotomic mapping $f_{a_0, a_1, \dots, a_{\ell-1}}^r$ such that none of a_i 's is zero. Moreover, in Theorem 2, we show that this distribution is asymptotically normal.

In Section 4, we study any random r -th order cyclotomic mapping polynomial by choosing a_i 's in Equation (3) independently at random

from \mathbb{F}_q . The probability distribution of value set size is given in Theorem 3. As a consequence, for $\ell = q - 1$, we obtain the exact probability distribution of the value set size of a random polynomial over \mathbb{F}_q with degree at most $q - 1$. In particular, we have the following corollaries to Theorem 3.

Corollary 1. *Let $g(x)$ be a random polynomial of degree at most $q - 1$ over \mathbb{F}_q with $g(0) = 0$. Then*

$$\mathbb{P}(|V_g| = k + 1) = \binom{q-1}{k} \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} \left(\frac{1+j}{q}\right)^{q-1}.$$

Consequently, for $k = o(q)$, we have

$$\mathbb{P}(|V_g| = k + 1) \sim \frac{1}{k!} (q-1)^k \left(\frac{k+1}{q}\right)^{q-1}.$$

This proves that if $k > 1$ is small compared to q then the number of polynomials over \mathbb{F}_q with degree less than or equal to $q - 1$ such that the value set size is k is always exponential in q . Moreover, we have

Corollary 2. *Let $g(x)$ be any random polynomial of degree at most $q - 1$ over finite field \mathbb{F}_q with $g(0) = 0$. Let $Y_q = q - |g(\mathbb{F}_q)|$ denote the number of missing nonzero values in the value set of g . Let $\mu_q = q/e$ and $\sigma_q^2 = (e^{-1} - 2e^{-2})q$. Then the distribution of $(Y_q - \mu_q)/\sigma_q$ tends to the standard normal, as $q \rightarrow \infty$.*

Finally in Section 5 we study a variation of our model used in Section 3. We consider the case when each subset A_i is chosen uniformly at random from all m_i -subsets of a given n -set for $i = 1, \dots, \ell$. This extends a result by Barot and Peña [4] and David [9]. We also show that the size of the complement of $\cup_{i=1}^{\ell} A_i$ is asymptotically normal.

2. METHODOLOGY

In [16], we obtained the following formula for the cardinality of the value set for an arbitrary polynomial.

Proposition 1 (Proposition 2.3 in [16]). *Let $g(x) = ax^r f(x^s) + b$ ($a \neq 0$) be any polynomial over \mathbb{F}_q with index $\ell = \frac{q-1}{s}$ and let $\gcd(r, s) = t$. Let γ be a fixed primitive element of \mathbb{F}_q . Then*

$$|V_g| = c \frac{s}{t} + 1, \text{ or } |V_g| = (c-1) \frac{s}{t} + 1,$$

where $c = |\{(\gamma^{ir} f(\gamma^{si}))^{s/t} \mid i = 0, \dots, \ell - 1\}|$.

As discussed earlier, it is sufficient to assume that $a = 1$ and $b = 0$ in Proposition 1. That is, we can view $g(x)$ as a r -th order cyclotomic mapping polynomial with the least index ℓ . In this case, we have $g(x) = a_i x^r$ when $x \in C_i$, where $a_i = f(\gamma^{si})$ for $i = 0, \dots, \ell - 1$. Recall that C_0 is the subgroup of \mathbb{F}_q^* consisting of all the ℓ -th powers of \mathbb{F}_q^* and we let T_0 be the subgroup of \mathbb{F}_q^* consisting of all the $t\ell$ -th powers. Hence T_i with $0 \leq i \leq t\ell - 1$ give all the cyclotomic cosets of index $t\ell$. We also note that x^r maps C_0 onto T_0 which contains $\frac{s}{t}$ distinct elements. So x^r maps each coset $C_i = \gamma^i C_0$ onto $\gamma^{ir} T_0$. Therefore g maps C_i onto $\gamma^{ir} f(\gamma^{si}) T_0$, which could be either the set $\{0\}$ (if $a_i = f(\gamma^{si}) = 0$) or one of the nonzero cyclotomic cosets of index $t\ell$. We observe that c is the number of distinct cyclotomic cosets of the form $\gamma^{ir} f(\gamma^{si}) T_0$, possibly along with the subset $\{0\}$ if one of a_i 's is zero. Hence we have $|V_g| = c \frac{s}{t} + 1$ or $(c - 1) \frac{s}{t} + 1$, the latter happens when some of a_i 's in $g(x) = a_i x^r$ equal 0.

Therefore the value set problem for a random r -th order cyclotomic mapping polynomial (or random polynomial) g , essentially requires us to study the number c in Proposition 1, the size of union of some cyclotomic cosets and possibly the subset $\{0\}$ if a_i 's take zero. More specifically, for $0 \leq i \leq \ell - 1$, each C_i is mapped to $A_{i+1} = g(C_i)$ which is one of $T_0, \dots, T_{t\ell-1}$ or $\{0\}$. Then c is the number of distinct A_j 's ($1 \leq j \leq \ell$) and the value set size is either $c \frac{s}{t} + 1$ or $(c - 1) \frac{s}{t} + 1$. More generally, we are interested in the distribution of the random variable $X_{t\ell} = |\cup_{j=1}^{\ell} A_j|$, while A_j are chosen independently according to a given distribution depending on that a_i is chosen independently at random from \mathbb{F}_q . Similar problems have been studied in [4, 9] when each A_j is chosen uniformly at random from all k -subsets of a given n -set.

Let $n = t\ell$ and let $D_0 = \{0\}$ and $D_j = T_{j-1}$ for $1 \leq j \leq t\ell - 1$. Let Y_n be the the number of D_1, \dots, D_{n-1} which are not in $\cup_{j=1}^{\ell} A_j$ for a random r -th order cyclotomic mapping polynomial with index ℓ such that $(r, s) = t$. We will derive exact probability distributions of Y_n and show that they are asymptotically normal. Throughout the paper, we shall use $(Y_n)_k$ to denote the falling factorial $Y_n(Y_n - 1)(Y_n - 2) \cdots (Y_n - k + 1)$. We use \mathbb{P} , \mathbb{E} , \mathbb{V} to denote the probability, expectation, and variance of a random variable, respectively.

The main tool for deriving the probability distribution of Y_n in the paper is through the sieve method and the falling factorial moments. Let B_1, \dots, B_n be n events in a probability space and $\mathcal{N} = \{1, \dots, n\}$. We note that $\mathbb{P}(Y_n = k)$ is the probability that exactly k of the B_j

occur. Define

$$S_h = \sum_{J \subset \mathcal{N}, |J|=h} \mathbb{P}(\cap_{j \in J} B_j).$$

Then the well-known sieve formula (See e.g. [5, Theorem 10]) gives

$$(4) \quad \mathbb{P}(Y_n = k) = \sum_{h=k}^n (-1)^{h-k} \binom{h}{k} S_h,$$

$$(5) \quad S_k = \sum_{h=k}^n \binom{h}{k} \mathbb{P}(Y_n = h).$$

Hence

$$(6) \quad \mathbb{E}((Y_n)_k) = k! S_k.$$

We also need the following result [12, Theorem 1] in order to show that Y_n is asymptotically normal.

Lemma 1. *Let $s_n > -\mu_n^{-1}$ and*

$$\sigma_n = \sqrt{\mu_n + \mu_n^2 s_n},$$

where $\mu_n \rightarrow \infty$ as $n \rightarrow \infty$. Suppose that

$$\mu_n = o(\sigma_n^3),$$

and a sequence Y_n of nonnegative random variables satisfies

$$\mathbb{E}((Y_n)_k) \sim \mu_n^k \exp\left(\frac{k^2 s_n}{2}\right),$$

uniformly for all integers k in the range $c\mu_n/\sigma_n \leq k \leq c'\mu_n/\sigma_n$ for some constants $c' > c > 0$. Then $(Y_n - \mu_n)/\sigma_n$ tends in distribution to the standard normal as $n \rightarrow \infty$.

3. SIZES OF VALUE SETS OF CYCLOTOMIC MAPPING POLYNOMIALS WITH NONZERO BRANCHES

In this section, we study of the value set size of a random r -th order cyclotomic mapping polynomial with nonzero branches (i.e., none of a_i 's is zero). This means that we choose a_i in (3) independently at random from \mathbb{F}_q^* and it leads to the following model. Let $n = t\ell$ and $D_1, D_2, \dots, D_{t\ell}$ be pairwise disjoint subsets of \mathbb{F}_q^* such that $|D_i| = s/t$ for all $1 \leq i \leq t\ell$. Because a_i is chosen independently at random from \mathbb{F}_q^* , this means that A_1, A_2, \dots, A_ℓ are chosen independently and uniformly at random from $\{D_1, D_2, \dots, D_{t\ell}\}$. We are interested in the distribution of $X_n = |\cup_{j=1}^\ell A_j|$. This is closely related to the distributions of ℓ labeled balls into $t\ell$ labeled boxes. Let Y_n be the number of empty boxes in a

random distribution of ℓ labeled balls into $t\ell$ labeled boxes. We note $X_n = n - (s/t)Y_n$. We first prove the following

Theorem 1. *Let Y_n be the number of empty boxes in a random distribution of ℓ labeled balls into $n = t\ell$ labeled boxes. We have*

$$\begin{aligned}\mathbb{E}((Y_n)_k) &= (t\ell)_k \left(\frac{t\ell - k}{t\ell} \right)^\ell, \\ \mathbb{P}(Y_n = k) &= \binom{t\ell}{k} \frac{1}{(t\ell)^\ell} \sum_{j=1}^{t\ell-k} (-1)^{t\ell-k-j} \binom{t\ell - k}{j} j^\ell.\end{aligned}$$

Proof Let $\mathcal{N} = \{1, 2, \dots, t\ell\}$. Let B_j be the event that box j is empty. We have

$$S_k = \sum_{J \subset \mathcal{N}, |J|=k} \mathbb{P}(\cap_{j \in J} B_j) = \binom{t\ell}{k} \mathbb{P}(\cap_{j=1}^k B_j) = \binom{t\ell}{k} \left(\frac{t\ell - k}{t\ell} \right)^\ell.$$

It follows from (6) that

$$\mathbb{E}((Y_n)_k) = (t\ell)_k \left(\frac{t\ell - k}{t\ell} \right)^\ell.$$

Using Equation (4), we obtain

$$\begin{aligned}\mathbb{P}(Y_n = k) &= \sum_{h=k}^n (-1)^{h-k} \binom{h}{k} S_h \\ &= \sum_{h=k}^{t\ell} (-1)^{h-k} \binom{h}{k} \binom{t\ell}{h} \left(\frac{t\ell - h}{t\ell} \right)^\ell \\ &= \binom{t\ell}{k} \sum_{h=k}^{t\ell} (-1)^{h-k} \binom{t\ell - k}{h - k} \left(\frac{t\ell - h}{t\ell} \right)^\ell \\ &= \binom{t\ell}{k} \frac{1}{(t\ell)^\ell} \sum_{j=0}^{t\ell-k} (-1)^{t\ell-j-k} \binom{t\ell - k}{j} j^\ell\end{aligned}$$

□

Next we obtain

Theorem 2. *Suppose $t = o(\ell^{1/5})$ as $n = t\ell \rightarrow \infty$. Define*

$$\mu_n = te^{-1/t}\ell, \quad \sigma_n^2 = te^{-2/t}(e^{1/t} - 1 - 1/t)\ell.$$

Then the distribution of $(Y_n - \mu_n)/\sigma_n$ tends to the standard normal, as $n \rightarrow \infty$.

Proof From Theorem 1, we have, as $\ell \rightarrow \infty$,

$$\begin{aligned}
\mathbb{E}(Y_n) &= t\ell \left(1 - \frac{1}{t\ell}\right)^\ell \\
&= t\ell \exp\left(\ell \ln\left(1 - \frac{1}{t\ell}\right)\right) \\
&= t\ell \exp\left(-\ell \left(\frac{1}{t\ell} + \frac{1}{2t^2\ell^2} + O\left(\frac{1}{(t\ell)^3}\right)\right)\right) \\
&= t\ell \exp\left(-\frac{1}{t} - \frac{1}{2t^2\ell} + O\left(\frac{1}{t^3\ell^2}\right)\right) \\
&\sim \mu_n,
\end{aligned}
\tag{7}$$

$$\begin{aligned}
\mathbb{V}(Y_n) &= \mathbb{E}(Y_n(Y_n - 1)) + \mathbb{E}(Y_n) - (\mathbb{E}(Y_n))^2 \\
&= (t\ell)(t\ell - 1) \left(1 - \frac{2}{t\ell}\right)^\ell + t\ell \left(1 - \frac{1}{t\ell}\right)^\ell - (t\ell)^2 \left(1 - \frac{1}{t\ell}\right)^{2\ell} \\
&= (t\ell)(t\ell - 1) \exp\left(\ell \ln\left(1 - \frac{2}{t\ell}\right)\right) + t\ell \exp\left(\ell \ln\left(1 - \frac{1}{t\ell}\right)\right) \\
&\quad - (t\ell)^2 \exp\left(2\ell \ln\left(1 - \frac{1}{t\ell}\right)\right) \\
&= (t\ell)(t\ell - 1) \exp\left(-\ell \left(\frac{2}{t\ell} + \frac{2}{(t\ell)^2} + O\left(\left(\frac{2}{t\ell}\right)^3\right)\right)\right) \\
&\quad + t\ell \exp\left(-\ell \left(\frac{1}{t\ell} + \frac{1}{2(t\ell)^2} + O\left(\left(\frac{1}{t\ell}\right)^3\right)\right)\right) \\
&\quad - (t\ell)^2 \exp\left(-2\ell \left(\frac{1}{t\ell} + \frac{1}{2(t\ell)^2} + O\left(\left(\frac{1}{t\ell}\right)^3\right)\right)\right) \\
&= (t\ell)(t\ell - 1) \exp\left(-\ell \left(\frac{2}{t\ell}\right)\right) \exp\left(-\frac{2\ell}{(t\ell)^2} + O\left(\left(\frac{2}{t\ell}\right)^3\right)\right) \\
&\quad + t\ell \exp\left(-\ell \left(\frac{1}{t\ell}\right)\right) \exp\left(-\frac{\ell}{2(t\ell)^2} + O\left(\left(\frac{1}{t\ell}\right)^3\right)\right) \\
&\quad - (t\ell)^2 \exp\left(-2\ell \left(\frac{1}{t\ell}\right)\right) \exp\left(-\frac{\ell}{(t\ell)^2} + O\left(\left(\frac{1}{t\ell}\right)^3\right)\right)
\end{aligned}
\tag{8}$$

$$\begin{aligned}
& \sim (t\ell)(t\ell - 1) \exp\left(-\ell \left(\frac{2}{t\ell}\right)\right) \left(1 - \frac{2\ell}{(t\ell)^2}\right) \\
& \quad + t\ell \exp\left(-\ell \left(\frac{1}{t\ell}\right)\right) \left(1 - \frac{\ell}{2(t\ell)^2}\right) \\
& \quad - (t\ell)^2 \exp\left(-2\ell \left(\frac{1}{t\ell}\right)\right) \left(1 - \frac{\ell}{(t\ell)^2}\right) \\
& \sim t\ell e^{-\frac{1}{t}} - t\ell e^{-\frac{2}{t}} - \ell e^{-\frac{2}{t}} \\
(9) \quad & \sim \sigma_n^2.
\end{aligned}$$

Under the assumption that $t = o(\ell^{1/5})$, we can verify that $\frac{\mu_n^2}{\sigma_n^6} \rightarrow 0$ as $n \rightarrow \infty$. We note μ_n/σ_n is of the order $\sqrt{t^3\ell}$. Hence for k in the range specified in Lemma 1, we have $k^2 = O(t^3\ell)$. Therefore

$$\begin{aligned}
(t\ell)_k &= (t\ell)^k \prod_{j=1}^{k-1} \left(1 - \frac{j}{t\ell}\right) \\
&= (t\ell)^k \exp\left(\sum_{j=1}^{k-1} \ln\left(1 - \frac{j}{t\ell}\right)\right) \\
&= (t\ell)^k \exp\left(-\sum_{j=1}^{k-1} \left(\frac{j}{t\ell} + \frac{j^2}{2t^2\ell^2} + O\left(\frac{j^3}{t^3\ell^3}\right)\right)\right) \\
&\sim (t\ell)^k \exp\left(-\frac{k^2}{2t\ell}\right), \\
\left(\frac{t\ell - k}{t\ell}\right)^\ell &= \exp\left(\ell \ln\left(1 - \frac{k}{t\ell}\right)\right) \\
&= \exp\left(-\ell \left(\frac{k}{t\ell} + \frac{k^2}{2t^2\ell^2} + O\left(\frac{k^3}{t^3\ell^3}\right)\right)\right) \\
&\sim \exp\left(-\frac{k}{t} - \frac{k^2}{2t^2\ell}\right).
\end{aligned}$$

It follows from (6) and (7) that

$$\mathbb{E}((Y_n)_k) \sim (t\ell)^k \exp\left(-\frac{k}{t} - \frac{k^2}{2t\ell} - \frac{k^2}{2t^2\ell}\right) \sim \mu_n^k \exp\left(-\frac{k^2(t+1)}{2t^2\ell}\right).$$

Now the result follows from Lemma 1 and the estimation

$$s_n = \frac{\sigma_n^2 - \mu_n}{\mu_n^2} = \frac{\mathbb{E}(Y_n(Y_n - 1))}{\mu_n^2} - 1 = -\frac{1}{t\ell} - \frac{1}{t^2\ell} + O\left(\frac{1}{t^2\ell^2}\right) > -\mu_n^{-1},$$

as $\frac{t}{\ell} \rightarrow 0$ when $\ell \rightarrow \infty$. \square

The following corollary follows immediately from Theorem 1, by noting $s = t = 1$ and $X_n = n - Y_n$.

Corollary 3. *Under the assumption of Theorem 1 and $X_n = n - Y_n$, we have*

$$\mathbb{P}(X_n = h) = \frac{1}{n^n} \binom{n}{h} \sum_{j=1}^h (-1)^{h-j} \binom{h}{j} j^n.$$

In particular,

$$\mathbb{P}(X_n = n) = \frac{n!}{n^n},$$

and for $h = o(n)$,

$$\mathbb{P}(X_n = h) \sim \frac{1}{h!} n^h \left(\frac{h}{n} \right)^n.$$

Consider $\ell = n = q - 1$ and $t = 1$. Because an r -th order cyclotomic mapping polynomial $f_{a_0, \dots, a_{q-2}}^r(x)$ always maps 0 to 0, Corollary 3 implies

Corollary 4. *Let $g(x)$ be any random r -th order cyclotomic mapping polynomial $f_{a_0, \dots, a_{q-2}}^r(x)$ over finite field \mathbb{F}_q such that none of a_i 's is zero. Then the probability of $|V_f| = h + 1$ is given by*

$$\mathbb{P}(X_{q-1} = h) = \frac{1}{(q-1)^{q-1}} \binom{q-1}{h} \sum_{j=1}^h (-1)^{h-j} \binom{h}{j} j^{q-1}.$$

In particular, the probability of such a random cyclotomic mapping polynomial $f_{a_0, \dots, a_{q-2}}^r(x)$ is a permutation polynomial is

$$\mathbb{P}(X_{q-1} = q - 1) = \frac{(q-1)!}{(q-1)^{q-1}},$$

and for $h = o(q)$, the probability of such a random cyclotomic mapping polynomial $f_{a_0, \dots, a_{q-2}}^r(x)$ with a value set size $h + 1$ is

$$\mathbb{P}(X_{q-1} = h) \sim \frac{1}{h!} (q-1)^h \left(\frac{h}{q-1} \right)^{q-1}.$$

4. SIZES OF VALUE SETS OF RANDOM POLYNOMIALS

Recall $q - 1 = \ell s$ and r is a positive integer such that $(r, s) = t$. In this section we consider the value set size for any random r -th order cyclotomic mapping polynomial $f_{a_0, \dots, a_{\ell-1}}^r(x)$ with index ℓ over finite field \mathbb{F}_q . Namely, $a_0, \dots, a_{\ell-1}$ are independently chosen at random from \mathbb{F}_q . We note that the value set problem for any random polynomial with

degree at most $q - 1$ is in fact the value set problem for a random r -th order cyclotomic mapping polynomial with index $\ell = q - 1$.

As discussed in Section 2, we are interested in the distribution of $X_n = |\cup_{j=1}^{\ell} A_j|$. However, we need to include the element 0 in our analysis similar to those in Section 3. Because each a_i in (3) is chosen independently at random from \mathbb{F}_q , this leads to the following model.

Let us define $D_0 = \{0\}$ and $D_j = T_{j-1}$ for $1 \leq j \leq t\ell$. The distribution of each random set A_i is $\mathbb{P}(A_i = D_0) = \frac{1}{q}$, and

$$\mathbb{P}(A_i = D_j) = \frac{1}{t\ell} \left(1 - \frac{1}{q}\right) = \frac{s}{tq}, \quad j = 1, \dots, \ell.$$

As in the case discussed earlier, we define the events $B_j = \cap_{i=1}^{\ell} \{A_i \neq D_j\}$, $0 \leq j \leq t\ell$. Let $Y_{t\ell}$ be the number of $B_1, B_2, \dots, B_{t\ell}$ (note B_0 is excluded) which occur. Then $\mathbb{P}(Y_{t\ell} = k)$ is the probability that exactly k of $t\ell$ cyclotomic sets T_j 's of index $t\ell$ are not in the value set of g . Then we have

Lemma 2. *Let $q - 1 = \ell s$ and r be a positive integer such that $(r, s) = t$. Let $g(x)$ be any random r -th order cyclotomic mapping polynomial $f_{a_0, \dots, a_{\ell-1}}^r(x)$ with index ℓ over finite field \mathbb{F}_q . Let $Y_{t\ell}$ be the number of cyclotomic sets of index $t\ell$ not contained in the value set of g . Then*

$$\begin{aligned} \mathbb{E}((Y_{t\ell})_k) &= (t\ell)_k \left(1 - \frac{sk}{tq}\right)^{\ell}, \\ \mathbb{P}(Y_{t\ell} = k) &= \binom{t\ell}{k} \sum_{j=0}^{t\ell-k} (-1)^{t\ell-j-k} \binom{t\ell-k}{j} \left(\frac{1}{q} + \frac{sj}{tq}\right)^{\ell}. \end{aligned}$$

Proof Let $\mathcal{N} = \{1, 2, \dots, t\ell\}$. Define

$$S_k = \sum_{J \subset \mathcal{N}, |J|=k} \mathbb{P}(\cap_{j \in J} B_j).$$

Because A_1, \dots, A_{ℓ} are mutually independent, we have

$$S_k = \binom{t\ell}{k} \mathbb{P}(\cap_{j=1}^k B_j) = \binom{t\ell}{k} \left(\frac{1}{q} + \frac{s(t\ell-k)}{tq}\right)^{\ell} = \binom{t\ell}{k} \left(1 - \frac{sk}{tq}\right)^{\ell}.$$

Using Equation (4), we obtain

$$\begin{aligned}
\mathbb{P}(Y_{t\ell} = k) &= \sum_{h=k}^{t\ell} (-1)^{h-k} \binom{h}{k} S_h \\
&= \sum_{h=k}^{t\ell} (-1)^{h-k} \binom{h}{k} \binom{t\ell}{h} \left(\frac{1}{q} + \frac{s(t\ell - h)}{tq} \right)^\ell \\
&= \binom{t\ell}{k} \sum_{h=k}^{t\ell} (-1)^{h-k} \binom{t\ell - k}{h - k} \left(\frac{1}{q} + \frac{s(t\ell - h)}{tq} \right)^\ell \\
&= \binom{t\ell}{k} \sum_{j=0}^{t\ell - k} (-1)^{t\ell - j - k} \binom{t\ell - k}{j} \left(\frac{1}{q} + \frac{sj}{tq} \right)^\ell.
\end{aligned}$$

□

Using the above lemma, we can obtain the distribution of $X_{t\ell} = |V_g|$.

Theorem 3. *Let $q - 1 = \ell s$ and r be a positive integer such that $(r, s) = t$. Let $f(x)$ be any random r -th order cyclotomic mapping polynomial $f_{a_0, \dots, a_{\ell-1}}^r(x)$ with index ℓ over \mathbb{F}_q . Then*

$$\mathbb{P}(X_{t\ell} = 1 + ks/t) = \binom{t\ell}{k} \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} \left(\frac{1}{q} + \frac{sj}{tq} \right)^\ell.$$

Proof Indeed,

$$\begin{aligned}
\mathbb{P}(X_{t\ell} = 1 + ks/t) &= \mathbb{P}(\{Y_{t\ell} = t\ell - k\}) \\
&= \binom{t\ell}{k} \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} \left(\frac{1}{q} + \frac{sj}{tq} \right)^\ell.
\end{aligned}$$

We now obtain an application of the above results on random polynomials with degree at most $q - 1$. It is sufficient to study the distribution of the subclass of random polynomials $g(x)$ such that $g(0) = 0$ with degree $\leq q - 1$, because any polynomial $f(x)$ such that $f(0) = b$ can be written as $g(x) + b$ with $g(0) = 0$ and vice versa. So we can view any random polynomial g of degree at most $q - 1$ with $g(0) = 0$ and index ℓ as an r -th order cyclotomic mapping polynomial with the least index ℓ , which is therefore a cyclotomic mapping polynomial with index $q - 1$. Because there are q^{q-1} such polynomials with $g(0) = 0$, they correspond to all the cyclotomic mapping polynomials with index $q - 1$. So a random polynomial with degree less than or equal to $q - 1$ and $g(0) = 0$ is a random r -th order cyclotomic mapping polynomial with index $\ell = q - 1$ for any $r \geq 1$. Therefore, Lemma 2 implies that any random polynomial with degree $q - 1$ has expected value set size

$(1 - \frac{1}{q})^{q-1} \sim \frac{q}{e}$. This verifies William's result [24] saying that almost all the polynomials of degree $q - 1$ is a general polynomial. Moreover, applying Theorem 3 to the case $\ell = q - 1$ (hence $s = t = 1$), we obtain exact probability distribution of the value set size for a random polynomial over finite field \mathbb{F}_q in Corollary 1. Moreover, we can drive Corollary 2 that the distribution of $(Y_{t\ell} - u_{t\ell})/\sigma_{t\ell}$ tends to the standard normal distribution as well, as $\ell \rightarrow \infty$ and $t = o(\ell^{1/5})$, following the same arguments as in the proof of Theorem 2.

5. SIZE OF THE UNION OF RANDOM SETS

Recall $\mathcal{N} = \{1, \dots, n\}$. In Section 3, we considered $|\cup_{i=1}^{\ell} A_i|$ where each A_i a random cyclotomic cosets of index ℓ . In Section 4, we allowed the possibility that A_i could be $\{0\}$, a subset with a different size from cyclotomic cosets. Earlier, Barot and Peña [4] considered the probability distribution of $|\cup_{i=1}^{\ell} A_i|$ where each A_i is chosen independently and uniformly at random from \mathcal{P}_m where \mathcal{P}_m is the set of all m -subsets of \mathcal{N} . In this section, we consider $|\cup_{i=1}^{\ell} A_i|$ such that m_i 's can be distinct. Let $X_n = |\cup_{i=1}^{\ell} A_i|$ and $Y_n = n - X_n$. In the following we establish the distributions of X_n and Y_n and we show that the Y_n is asymptotically normal. This generalizes the following result by Barot and Peña [4] because we allow m_i 's to be distinct.

Theorem 4 (Barot and Peña, 2001). *Let $\mathcal{N} = \{1, \dots, n\}$. Let $X_n = |\cup_{i=1}^{\ell} A_i|$ where each A_i is chosen independently and uniformly at random from \mathcal{P}_m where \mathcal{P}_m is the set of all m -subsets of \mathcal{N} and $Y_n = n - X_n$. We have*

$$\begin{aligned} \mathbb{P}(X_n = i) &= \frac{\binom{n}{i}}{\binom{n}{m}^{\ell}} \sum_{j=0}^{i-m} (-1)^j \binom{i}{j} \binom{i-j}{m}^{\ell}, \\ \mathbb{E}(X_n) &= n \left(1 - \left(1 - \frac{m}{n} \right)^{\ell} \right), \\ \mathbb{V}(X_n) &= n(n-1) \left(1 - \frac{m}{n} \right)^{\ell} \left(1 - \frac{m}{n-1} \right)^{\ell} - (\mathbb{E}(X_n))^2 + \mathbb{E}(X_n). \end{aligned}$$

First of all, we extend the above results to general m_i 's.

Lemma 3. *Let $\mathcal{N} = \{1, \dots, n\}$ and \mathcal{P}_{m_i} be the set of all m_i -subsets of \mathcal{N} for $1 \leq i \leq \ell$. Let X_n be the random variable for the size of $\cup_{i=1}^{\ell} A_i$ where A_i is a random set chosen independently and uniformly*

from \mathcal{P}_{m_i} and $Y_n = n - X_n$. We have

$$(10) \quad \mathbb{E}((Y_n)_k) = (n)_k \prod_{j=1}^{\ell} \frac{(n - m_j)_k}{(n)_k},$$

$$(11) \quad \mathbb{P}(Y_n = k) = \sum_{h=k}^n (-1)^{h-k} \binom{h}{k} \binom{n}{h} \prod_{j=1}^{\ell} \frac{(n - m_j)_h}{(n)_h},$$

$$(12) \quad \mathbb{P}(X_n = i) = \binom{n}{i} \sum_{h=0}^i (-1)^h \binom{i}{h} \prod_{j=1}^{\ell} \frac{\binom{i-h}{m_j}}{\binom{n}{m_j}}.$$

Proof For each $j \in \mathcal{N}$, let B_j denote the event that $j \notin \cap_{i=1}^{\ell} A_i$. We note that $\mathbb{P}(Y_n = k)$ is the probability that exactly k of the B_j 's occur. Since $A_1, A_2, \dots, A_{\ell}$ are mutually independent, we have

$$\begin{aligned} S_k &= \binom{n}{k} \mathbb{P}(B_1 \cap B_2 \cap \dots \cap B_k) \\ &= \binom{n}{k} \prod_{j=1}^{\ell} \mathbb{P}(1 \notin A_j, 2 \notin A_j, \dots, k \notin A_j) \\ &= \binom{n}{k} \prod_{j=1}^{\ell} \frac{(n - m_j)_k}{(n)_k}, \end{aligned}$$

and hence

$$\mathbb{E}((Y_n)_k) = k! S_k = (n)_k \prod_{j=1}^{\ell} \frac{(n - m_j)_k}{(n)_k}.$$

Now from (4) we obtain $\mathbb{P}(Y_n = k) = \sum_{h=k}^n (-1)^{h-k} \binom{h}{k} \binom{n}{h} \prod_{j=1}^{\ell} \frac{(n - m_j)_h}{(n)_h}$. Finally,

$$\begin{aligned} \mathbb{P}(X_n = i) &= \mathbb{P}(Y_n = n - i) \\ &= \sum_{h=n-i}^n (-1)^{h-n+i} \binom{h}{n-i} \binom{n}{h} \prod_{j=1}^{\ell} \frac{(n - m_j)_h}{(n)_h} \\ &= \binom{n}{i} \sum_{h=0}^i (-1)^h \binom{i}{h} \prod_{j=1}^{\ell} \frac{\binom{i-h}{m_j}}{\binom{n}{m_j}}, \end{aligned}$$

where the last equality holds after the substitution $h := h - n + i$. \square .

Next we show that Y_n is asymptotically normal. The condition on u_i in the following theorem can be relaxed considerably, but we use the current form for the sake of simplicity.

Theorem 5. *Let $u_j = m_j/n$. Suppose $\ell \rightarrow \infty$, $u_j = O(1/\ell)$ uniformly for all $1 \leq j \leq \ell$, and $\sum_{i=1}^{\ell} u_i > c$ for some positive constant c . Then Y_n is asymptotically normal with mean and variance, respectively, equal to*

$$\begin{aligned}\mu_n &= n \prod_{i=1}^{\ell} (1 - u_i), \\ \sigma_n^2 &= n \left(1 - \left(1 + \sum_{i=1}^{\ell} u_i \right) \prod_{i=1}^{\ell} (1 - u_i) \right) \prod_{i=1}^{\ell} (1 - u_i).\end{aligned}$$

Proof For $k = O(\sqrt{n})$, We have

$$\begin{aligned}\mathbb{E}((Y_n)_k) &= (n)_k \prod_{i=1}^{\ell} \frac{(n - m_i)_k}{(n)_k} \\ &= n^k \exp \left(-\frac{k(k-1)}{2n} + O\left(\frac{k^3}{n^2}\right) \right) \prod_{i=1}^{\ell} \prod_{j=0}^{k-1} \left(1 - u_i - \frac{ju_i}{n-j} \right) \\ &= \mu_n^k \exp \left(-\frac{k(k-1)}{2n} + O\left(\frac{k^3}{n^2}\right) \right) \prod_{i=1}^{\ell} \exp \left(\sum_{j=0}^{k-1} \ln \left(1 - \frac{ju_i}{(1-u_i)(n-j)} \right) \right) \\ &= \mu_n^k \exp \left(-\frac{k(k-1)}{2n} + O\left(\frac{k^3}{n^2}\right) - \sum_{i=1}^{\ell} \sum_{j=0}^{k-1} \frac{ju_i}{(1-u_i)(n-j)} \right) \\ &= \mu_n^k \exp \left(-\frac{k(k-1)}{2n} - \sum_{i=1}^{\ell} \sum_{j=0}^{k-1} \frac{ju_i}{(1-u_i)n} + O\left(\frac{k^3}{n^2}\right) \right) \quad (\text{because } j \leq k \sim \sqrt{n}) \\ &= \mu_n^k \exp \left(-\frac{k(k-1)}{2n} \left(1 + \sum_{i=1}^{\ell} u_i \right) + O\left(\frac{k^3}{n^2} + \frac{k^2}{n\ell}\right) \right). \quad (\text{note } u_j = O(1/\ell))\end{aligned}$$

In particular we have

$$\mathbb{E}((Y_n)_2) = \mu_n^2 \exp \left(-\frac{1}{n} \left(1 + \sum_{i=1}^{\ell} u_i \right) + O\left(\frac{1}{n^2} + \frac{1}{n\ell}\right) \right),$$

and for k of the order \sqrt{n} ,

$$\mathbb{E}((Y_n)_k) \sim \mu_n^k \exp \left(-\frac{k^2}{2n} \left(1 + \sum_{i=1}^{\ell} u_i \right) \right).$$

It follows that

$$\begin{aligned}
s_n &= \frac{\sigma_n^2 - \mu_n}{\mu_n^2} \\
&= \frac{\mathbb{E}(Y_n(Y_n - 1))}{\mu_n^2} - 1 \\
&= \exp\left(-\frac{1}{n}\left(1 + \sum_{i=1}^{\ell} u_i\right) + O\left(\frac{1}{n^2} + \frac{1}{n\ell}\right)\right) - 1 \\
&= -\frac{1}{n}\left(1 + \sum_{i=1}^{\ell} u_i\right) + O\left(\frac{1}{n^2} + \frac{1}{n\ell}\right),
\end{aligned}$$

and

$$\mathbb{E}((Y_n)_k) \sim \mu_n^k \exp\left(\frac{k^2 s_n}{2}\right).$$

Now the theorem follows from Lemma 1. \square

REFERENCES

- [1] A. Akbary, D. Ghioca, and Q. Wang, On permutation polynomials of prescribed shape, *Finite Fields Appl.* 15 (2009), 195-206.
- [2] B. J. Birch and H. P. F. Swinnerton-Dyer, Note on a problem of Chowla, *Acta Arith.* 5 (1959), 417-423.
- [3] H. Borges and R. Conceicao, On the characterization of minimal value set polynomials, *J. Number Theory* 133 (2013), 2021-2035.
- [4] M. Barot and J. Peña, Estimating the size of a union of random subsets of fixed cardinality, *Elemente der Mathematik* 56 (2001), no. 4, 163-169.
- [5] B. Bollobás, *Random Graphs*, Academic Press, 1985.
- [6] L. Carlitz, D. J. Lewis, W. H. Mills, and E. G. Straus, Polynomials over finite fields with minimal value sets, *Mathematika* 8 (1961), 121-130.
- [7] Q. Cheng, J. Hill and D. Wan, Counting value sets: algorithms and complexity, Tenth Algorithmic Number Theory Symposium ANTS-X, 2012, University of California at San Deigo.
- [8] S. D. Cohen, The distribution of polynomials over finite fields, *Acta Arith.* 17 (1970), 255-271.
- [9] F.N. David, *Biometrika* 37 (1950), 97-110.
- [10] P. Das and G. L. Mullen, Value sets of polynomials over finite fields, in *Finite Fields with Applications in Coding Theory, Cryptography and Related Areas*, G.L. Mullen, H. Stichtenoth, and H. Tapia-Recillas, Eds., Springer, 2002, 80-85.
- [11] A. B. Evans, Orthomorphism Graphs of Groups, *Lecture Notes in Mathematics*, Vol. 1535, Springer, Berlin, 1992.

- [12] Z. Gao and N.C. Wormald, Asymptotic normality determined by high moments, and submap counts of random maps, *Probab. Theory Relat. Fields* 130 (2004), 368-376.
- [13] J. Gomez-Calderon and D. J. Madden, Polynomials with small value set over finite fields, *J. Number Theory* 28 (1988), no. 2, 167-188.
- [14] R. Guralnick and D. Wan, Bounds for fixed point free elements in a transitive group and applications to curves over finite fields, *Israel J. Math.* 101 (1997), 255-287.
- [15] W. H. Mills, Polynomials with minimal value sets, *Pacific J. Math* 14 (1964), 225-241.
- [16] G. L. Mullen, D. Wan, and Q. Wang, Value sets of polynomial maps over finite fields, *Quart. J. Math.* 64 (2013), no. 4, 1191-1196.
- [17] G. L. Mullen, D. Wan, and Q. Wang, An index bound on value sets of polynomial maps over finite fields, *Proceedings of Workshop on the Occasion of Harald Niederreiter's 70th Birthday: Applications of Algebra and Number Theory*, June 23-27, 2014.
- [18] H. Niederreiter and A. Winterhof, Cyclotomic \mathcal{R} -orthomorphisms of finite fields, *Discrete Math.* 295 (2005), 161-171.
- [19] G. Turnwald, A new criterion for permutation polynomials, *Finite Fields Appl.* 1 (1995), 64-82.
- [20] D. Wan, A p -adic lifting lemma and its applications to permutation polynomials, *Lecture Notes in Pure and Appl. Math.*, Marcel Dekker, New York, Vol. 141, 1992, 209-216.
- [21] D. Wan, P. J. S. Shiue and C. S. Chen, Value sets of polynomials over finite fields, *Proc. Amer. Math. Soc.* 119 (1993), 711-717.
- [22] Q. Wang, *Cyclotomic mapping permutation polynomials over finite fields*, Sequences, Subsequences, and Consequences (International Workshop, SSC 2007, Los Angeles, CA, USA, May 31 - June 2, 2007), 119-128, *Lecture Notes in Comput. Sci.* Vol. 4893, Springer, Berlin, 2007.
- [23] Q. Wang, Cyclotomy and permutation polynomials of large indices, *Finite Fields Appl.* 22 (2013), 57-69.
- [24] K. S. Williams, On general polynomials, *Canad. Math. Bull.* 10 (1967), no. 4, 579-583.

SCHOOL OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY, 1125
 COLONEL BY DRIVE, OTTAWA, ON K1S 5B6, CANADA
E-mail address: zgao@math.carleton.ca, wang@math.carleton.ca